DLA PIPER US LLP
Roy K. McDonald (State Bar No. 193691)
roy.mcdonald@dlapiper.com
Stephen A. Chiari (State Bar No. 221410)
stephen.chiari@dlapiper.com
153 Townsend Street, Suite 800
San Francisco, California 94107-1957
Telephone: (415) 836-2547
Facsimile: (415) 659-7447

Attorneys for Plaintiffs
ECHOSTAR SATELLITE L.L.C.,
ECHOSTAR TECHNOLOGIES CORPORATION
and NAGRASTAR L.L.C.

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

ECHOSTAR SATELLITE L.L.C., a Colorado Limited Liability Company, ECHOSTAR TECHNOLOGIES CORPORATION, a Texas Corporation, and NAGRASTAR L.L.C., a Colorado Limited Liability Company,

Plaintiffs,

v.

FREETECH, INC., a California Corporation, and DOES 1-10,

Defendants.

Case No. CV 07 6124

PLAINTIFFS' COMPLAINT FOR:

1) **Violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(2);**

2) **Violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201(b)(1);**

3) **Violation of the Communications Act of 1934, as amended, 47 U.S.C. § 605(a);**

4) **Violation of the Communications Act of 1934, as amended, 47 U.S.C. § 605(e)(4);**

5) **Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2520(a);**

6) **Unfair Competition in Violation of California Business & Professions Code § 17200;**

7) **Unjust Enrichment.**

DEMAND FOR JURY TRIAL

Plaintiffs ECHOSTAR SATELLITE L.L.C., ECHOSTAR TECHNOLOGIES CORPORATION (collectively "ECHOSTAR"), and NAGRASTAR L.L.C. ("NAGRASTAR"), by their undersigned counsel, file this Original Complaint against the above-named Defendants and state as follows:

INTRODUCTION & NATURE OF THE ACTION

1. Plaintiffs ECHOSTAR and NAGRASTAR bring this action against Defendants FREETECH, INC. and DOES 1 through 10 (collectively "Defendants") for unlawfully manufacturing, distributing, and otherwise trafficking in devices, components, and technology intended to facilitate the illegal and unauthorized reception and decryption of ECHOSTAR's subscription and pay-per-view television programming.

2. ECHOSTAR is a multi-channel video provider, providing video, audio, and data services to customers throughout the United States, Puerto Rico, and the U.S. Virgin Islands via a Direct Broadcast Satellite ("DBS") system. ECHOSTAR uses high-powered satellites to broadcast, among other things, movies, sports, and general entertainment services ("Programming") to consumers who have been authorized to receive such services after payment of a subscription fee (or in the case of a pay-per-view movie or event, the purchase price).

3. ECHOSTAR operates its DBS Programming under the trade name "DISH Network." To provide customers with a variety of Programming channels, ECHOSTAR continues to contract and purchase the distribution rights of copyrighted Programming from providers such as network affiliates, pay and specialty broadcasters, cable networks, motion picture distributors, sports leagues, event promoters, and other content providers.

4. Because ECHOSTAR generates revenues through the sale of subscription packages and pay-per-view programming, and because the ability to attract and retain the distribution rights for Programming is dependent upon preventing the unauthorized reception of DISH Network Programming signals, all of ECHOSTAR's video channels, except for certain promotional channels, are digitally secured.

5. ECHOSTAR protects DISH Network Programming from unauthorized viewing by using a management and security system ("Security System"), which serves two interrelated

functions: (1) subscriber-management—allowing ECHOSTAR to "turn on" or "turn off" Programming that a customer ordered, cancelled, or changed; and (2) encryption—preventing individuals or entities who have not purchased DISH Network Programming from viewing it.

6. The Security System is comprised of two parts. First, ECHOSTAR encrypts (electronically scrambles) its satellite signals using proprietary technology provided by NAGRASTAR. Essentially, NAGRASTAR provides ECHOSTAR with "smart cards" ("Access Cards") that contain a microprocessor component that functions as a security computer to a "conditional access system" known as Digital Nagra Advanced Security Process ("DNASP"). These Access Cards are utilized in the satellite receivers that customers either purchase or lease. Second, the DNASP uses a complex encryption system that is combined with a Digital Video Broadcasting ("DVB") scrambler/encoding system to effectively protect and encrypt DISH Network Programming.

7. Defendants violated federal and state law by offering to the public, providing, or otherwise engaging in the traffic of devices, components, and technology that are primarily designed to circumvent and/or defeat Plaintiffs' Security System and ultimately facilitate the unauthorized reception of ECHOSTAR's encrypted satellite signals and DISH Network Programming.

PARTIES

8. Plaintiff ECHOSTAR SATELLITE L.L.C. is a Colorado limited liability company with its principal place of business located at 9601 South Meridian Blvd., Englewood, Colorado 80112.

9. Plaintiff ECHOSTAR TECHNOLOGIES CORPORATION is a Texas corporation with its principal place of business located at 90 Inverness Circle East, Englewood, Colorado 80112.

10. Plaintiff NAGRASTAR L.L.C. is a Colorado limited liability company with its principal place of business located at 90 Inverness Circle East, Englewood, Colorado 80112. NAGRASTAR is a joint venture between ECHOSTAR and the Kudelski Group, a group of companies headquartered in Switzerland.

11. Upon information and belief, Defendant FREETECH, INC. ("FREETECH") is a California corporation with its principal place of business located at 469 Littlefield Avenue, South San Francisco, California 94080. The registered agent for FREETECH is Heejoun Jin, 469 Littlefield Avenue, South San Francisco, California 94080.

12. The true names and capacities of Defendants DOES 1 through 10, whether individual, corporate, associate, or otherwise, are masked by monikers used on the Internet and thus unknown to Plaintiffs at this time. Plaintiffs believe that information obtained in discovery will lead to the identification of each Defendant's true name.

13. Upon information and belief, each of the Defendants, including DOES 1 through 10, was the agent and/or prinicipal for one another, was acting within the scope of such agency when engaging in the misconduct alleged herein, and is jointly and severally liable for all damages arising as a result thereof.

JURISDICTION AND VENUE

14. This is a civil action predicated upon violations of the Digital Millennium Copyright Act, 17 U.S.C. § 1201 *et seq.*, the Communications Act of 1934, as amended, 47 U.S.C. § 605 *et seq.*, and the Electronic Communications Privacy Act, 18 U.S.C. § 2511 *et seq.* Therefore, jurisdiction is proper in this Court pursuant to 28 U.S.C. §§ 1331, 1338, 47 U.S.C. § 605(e)(3)(A), 17 U.S.C. § 1203, and 18 U.S.C. § 2520(a). The Court has supplemental jurisdiction over the state law claims asserted herein pursuant to 28 U.S.C. § 1367(a).

15. Personal jurisdiction and venue are proper in this Court pursuant to 28 U.S.C. §§ 1391(b)(1) because at least one Defendant resides within this judicial district and the remaining Defendants reside in California, 1391(b)(2) because a substantial part of the events giving rise to this action occurred in this judicial district, 1391(b)(3) because Defendants may be found in this judicial district and are subject to *in personam* jurisdiction, and 1400(a) because this case asserts the infringement and circumvention of protected copyright materials.

PLAINTIFFS' SECURITY SYSTEM

16. A consumer wishing to subscribe to and receive DISH Network Programming must first have the necessary equipment, which consists primarily of: (1) a satellite dish antenna

("dish"); (2) an integrated receiver/decoder ("receiver" or "set-top box"); and (3) a credit card-sized ECHOSTAR Access Card.

17. A satellite dish can be mounted on a rooftop, deck railing, or other structure at the subscriber's home or business. After proper installation, the dish antenna will receive programming signals from one of ECHOSTAR's satellites, which are then transmitted by wire into the set-top box. The receiver processes and descrambles the incoming signal using the data and encryption technology stored in the ECHOSTAR Access Card. The Access Card is loaded into the receiver through a slot located at the face of the unit.

18. ECHOSTAR provides the Access Cards to customers for use with the receivers for the purpose of enabling authorized access to DISH Network Programming. Absent a subscription to DISH Network, ECHOSTAR will not provide a consumer an Access Card or authorize access to encrypted DISH Network Programming. Subscribers are not authorized to modify or tamper with the Access Card, which are clearly marked as property of ECHOSTAR and must be returned upon request.

19. The ECHOSTAR Access Card is essential to the operation of the set-top box because it contains a secure embedded microprocessor that essentially functions as a small security computer, with secret keys and software that contain technology codes ("Nagra Software") used to communicate with the receiver and enable the descrambling of DISH Network Programming. The Nagra Software and the security components contained in each set-top box are licensed from NAGRASTAR.

20. The Nagra Software within each Access Card is supported by two code segments of memory: (1) Read-Only-Memory ("ROM"); and (2) Electronically Erasable Programmable Read-Only-Memory ("EEPROM"). Generally, the ROM code segment contains the intimate knowledge and information regarding Plaintiffs' Security System and how it works; whereas the EEPROM code segment contains the secret keys enabling the decryption of ECHOSTAR's satellite signal.

21. The ROM code segment provides detailed instructions and commands to ECHOSTAR Access Cards and set-top boxes in the normal operation of Plaintiffs' Security

System. Access to the proprietary information stored in the ROM code is necessary to unlock the safe containing the secrets to Plaintiffs' Security System.

22. The EEPROM code segment stores data and command codes that have been written to ECHOSTAR Access Cards which the ROM code reads from to perform its calculation and operation functions. Moreover, the EEPROM code segment contains secret "transmission" keys and secret "pairing" keys (collectively known as "security keys"). The security keys are used to encrypt and decrypt the communications between the ECHOSTAR Access Card and the set-top box.

23. ECHOSTAR communicates with the microprocessor in each Access Card by sending and receiving satellite signals which are routinely updated. The information transmitted to and temporarily stored on the Access Card includes the most recent security keys and software necessary to view DISH Network Programming.

24. Plaintiffs' Security System effectively controls access to the copyrighted materials that comprise DISH Network Programming. In addition, the Security System ensures that the protection afforded to such copyrighted works, such as limitations on the dissemination and use in accordance with ECHOSTAR's contractual agreements with content providers, is preserved.

THE PIRACY OF DISH NETWORK PROGRAMMING

25. Upon information and belief, satellite pirates reverse engineered the Nagra Software in the ECHOSTAR Access Card. As a result, these pirates ultimately copied and acquired the proprietary information stored within the ROM and EEPROM code segments of the Access Card, and compromised Plaintiffs' Security System. The pirate community (commercial and consumer) used this knowledge to develop various types of devices and technology for the sole purpose of illegally descrambling or "pirating" DISH Network Programming.

26. To combat the piracy of DISH Network Programming, Plaintiffs periodically introduce new ECHOSTAR Access Cards that contain updated security codes and software. In addition, Plaintiffs continue to invest in the development and deployment of electronic countermeasures ("ECM") to maintain the integrity of the Security System. An ECM is a

command transmitted in the stream of data that targets Access Cards, or clones thereof, that are using known modified software code and disables those Access Cards.

THE SALE AND USE OF FREE-TO-AIR RECEIVERS FOR SATELLITE PIRACY

27. Despite the continuous improvements to Plaintiffs' Security System, satellite piracy continues to proliferate with the ever-growing access and popularity of the Internet. With the Internet as a sword, pirates developed a new way to steal DISH Network Programming by using so-called "free-to-air" receivers ("FTA Receivers"). FTA Receivers are devices that can receive "free-to-air" satellite television signals, which are either not scrambled or scrambled but available free of charge. "Free-to-air" channels do not offer the same type of popular programming found in subscription television packages (e.g. HBO, ESPN, etc.). Instead, "free-to-air" television channels typically include limited ethnic, religious, business, music, information, and advertising content.

28. FTA Receivers are similar to the receivers used by ECHOSTAR in that they are set-top boxes, approximately the size of a VCR player, which contain descrambling circuits and software that enables the units to perform designated functions. A variety of FTA Receivers are even equipped with an Access Card reader.

29. While FTA Receivers contain many of the same components found in an ECHOSTAR set-top box, the units cannot descramble and receive DISH Network Programming without utilizing the security keys and technology codes found in the Nagra Software (i.e. ROM code segment, EEPROM code segment). Upon information and belief, manufacturers of FTA Receivers developed firmware and components within each unit that will accept and receive illegal pirate software (hereinafter "Pirate Software") that contains the secret keys and codes to Plaintiffs' Security System. Once this technology is downloaded or "flashed" into the FTA Receiver, the unit will illegally receive DISH Network Programming.

30. Upon information and belief, the firmware and components within each FTA Receiver that enable the device to accept the download of illegal Pirate Software are (1) a capability that has been designed into each FTA Receiver specifically for Pirate Software; and (2) a capability that has no practical application other than to circumvent Plaintiffs' Security System.

31. Commercial pirates acquired, modified, and sold FTA Receivers by: (1) obtaining the FTA Receivers directly from their manufacturer or elsewhere; (2) loading or "flashing" the requisite Pirate Software onto the circuit chips or firmware contained within the FTA Receivers; (3) once "flashed" with the Pirate Software, "testing" the FTA Receivers to ensure the device would receive and descramble DISH Network Programming without authorization from or payment to ECHOSTAR; and (4) ultimately, selling the FTA Receivers to household consumer pirates on the Internet.

32. Upon information and belief, commercial pirates recently changed their approach by not actually loading the Pirate Software onto the FTA receivers themselves, but distributing the requisite piracy technology and information to select individuals on websites or Internet discussion "forums" who then offer the Pirate Software to consumers for download. These websites or forums are typically sponsored by many of the commercial pirates, who use this venue to advertise and tout their brand of FTA equipment. This approach, which is prevalent today, permits commercial pirates (including the manufacturers and distributors of FTA Receivers) to assert the misleading claim that they are distributing only "unprogrammed" or "unflashed" piracy devices to consumers.

33. In some cases, website forums provide and offer: (1) information and/or instruction, including sources of supply, production information, and product reviews; (2) discussion threads on topics of interest to the piracy community, including software "hacks" or "fixes" designed to restore functionality to ECHOSTAR Access Cards that have been disabled by Plaintiffs' countermeasures; (3) security keys for DISH Network Programming, which are necessary to unscramble programming from an FTA receiver; (4) piracy or "flashing" software files for download to their users; and (5) links and advertisements to other piracy websites that sell FTA Receivers, Pirate Software, or other piracy devices, components, and technology used to steal DISH Network Programming.

34. Successful forum sites can have thousands of members, and are often managed by certain users designated by the operating pirate(s) as "administrators" or "moderators." These individuals are typically given the authority to manage the content posted on the forum site.

Upon information and belief, the distributors of FTA Receivers provide equipment, updated piracy technology, and information to the administrators or moderators of select forums for distribution.

35. The distribution, sale, and use of FTA Receivers for piracy pose a serious threat to ECHOSTAR and NAGRASTAR. Inasmuch as FTA Receivers are not manufactured or sold by Plaintiffs to receive DISH Network Programming, neither ECHOSTAR nor NAGRASTAR can control or regulate the software contained in these devices. As a result, the ECMs traditionally used to combat satellite piracy may not be effective.

DEFENDANTS' WRONGFUL CONDUCT

36. Defendants directly, and through others acting in concert, distribute and promote the sale of "Coolsat" branded FTA Receivers throughout the United States. Upon information and belief, discovery will show that Defendants sold thousands of these FTA Receivers to consumer pirates for the sole purpose of circumventing Plaintiffs' Security System.

37. Similar to other FTA Receivers, it is believed that the satellite equipment distributed by Defendants contains computer firmware and components designed to accept the download of Pirate Software created solely for "Coolsat" branded FTA Receivers. Once flashed with this technology, these FTA Receivers can and will illegally receive DISH Network Programming.

38. Defendants import a variety of FTA Receivers from a manufacturer in Asia. Upon information and belief, discovery will show that this manufacturer not only creates the firmware and components within each device, but develops, designs, and updates the requisite Pirate Software with the assistance and support of Defendants.

39. Upon information and belief, discovery will show that FTA Receivers accept the download of illegal Pirate Software through internal firmware and components that (1) have been specifically designed to communicate with Pirate Software; and (2) have no commercially significant purpose or use other than to circumvent Plaintiffs' Security System.

40. Upon information and belief, discovery will also show that Defendants directly, and through others acting in concert, distribute the updated Pirate Software to select website

administrators and moderators, who then disseminate this technology to consumers on the Internet. Because Plaintiffs continue to develop technological measures that effectively control access to the copyrighted Programming on the DISH Network satellite platform, the demand for updated Pirate Software remains constant. As a result, the popularity of pirate websites and discussion forums continues to grow.

41. Defendants' authorized dealers purposefully advertise and promote "Coolsat" branded FTA Receivers on several well-known piracy websites. These websites not only provide consumers with illegal Pirate Software, but offer instruction and information used to unscramble and steal DISH Network Programming. Below are exemplars of typical hyperlink advertisements prominently displayed on pirate websites:

42. Upon information and belief, discovery will show that competition within the FTA industry is volatile and market share is contingent upon the immediate availability of updated Pirate Software. Distributors, such as FREETECH, are often pressured to provide consumer pirates with an immediate "fix" to combat a particular countermeasure or ECM utilized by Plaintiffs to prevent the unauthorized reception of DISH Network Programming. FREETECH is considered one of the industry leaders because of its commitment to immediately address the demands of the pirate community.

43. Upon information and belief, discovery will show that FREETECH developed the following process to expedite the design, development, and distribution of Pirate Software: (1) Defendants continuously monitor and intercept Plaintiffs' encrypted satellite signals to determine the deployment of an ECM; (2) Defendants immediately solicit information identifying the countermeasure commands transmitted in a particular ECM; (3) after Defendants acquire the requisite ECM data or "log" of coded commands (typically in "hexadecimal" format),

FREETECH then sends the information directly to coders in Asia; (4) the coders analyze the data and develop a "fix" or "patch" to the ECM; (5) the updated Pirate Software is then sent from the coders directly to FREETECH for testing; (6) if the updated Pirate Software effectively counters the ECM by allowing the user to circumvent Plaintiffs' Security System, FREETECH sends the "fix" to an individual known in the pirate community as "David Smith," "Tecknofreak," and "Matchstick" (collectively "Smith"); (7) Smith disseminates the updated Pirate Software through a fictitious entity or group of individuals known as the "Norwest Group" to several pirate websites, including www.fortecfiles.com, www.abadss.com, and www.f2atv.com.

44. Aside from the aforementioned design, development, and distribution, it is believed that FREETECH also utilizes Pirate Software to conduct diagnostic evaluations of FTA Receivers returned to FREETECH for reported warranty repair. Upon information and belief, discovery will show that FREETECH purposefully "flashes" or loads the most recent version of Pirate Software onto returned "Coolsat" FTA Receivers to determine why a particular unit is reportedly unable to receive DISH Network Programming. Once repaired, the Pirate Software is deleted from the FTA Receiver and the unit is returned to the customer, who is then directed to, or provided by Defendants, the updated Pirate Software for download.

CLAIMS FOR RELIEF

COUNT I

(Manufacture of and Traffic in Signal Theft Devices, Components, and Technology in Violation of the Digital Millennium Copyright Act, 17 U.S.C. §§ 1201(a)(2) and 1201(b)(1))

45. Plaintiffs incorporate by reference paragraphs 1 through 44 as if set forth herein.

46. Defendants were and are actively engaged in the business of manufacturing, importing, offering to the public, providing, or otherwise trafficking in the sale of illegal pirate devices, components, and technology in violation of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. §§ 1201(a)(2) and 1201(b)(1).

47. The FTA Receivers and corresponding Pirate Software provided by Defendants are: (1) designed or produced by Defendants primarily for the circumvention of Plaintiffs' Security System—a technological measure that effectively controls access to, copying and

distribution of, copyrighted works; (2) made available by Defendants despite having no limited commercially significant purpose or use other than to circumvent Plaintiffs' Security System; and/or (3) marketed by Defendants, or through others acting in concert, with knowledge that the devices, components, and technology are used to circumvent Plaintiffs' Security System.

48. Defendants were and are manufacturing, importing, offering to the public, providing, or otherwise trafficking "Coolsat" branded FTA Receivers and corresponding Pirate Software with knowledge that these devices, components, and technology are used to circumvent and defeat Plaintiffs' conditional access technological measures that protect the copyrighted works on the DISH Network satellite platform.

49. Defendants' actions that constitute violations of the DMCA were performed without the permission, authorization, or consent of ECHOSTAR, NAGRASTAR, or any owner of copyrighted Programming broadcast on the DISH Network platform.

50. Defendants violated sections 1201(a)(2) and 1201(b)(1) of the DMCA willfully and for purposes of commercial advantage or private financial gain.

51. Defendants' misconduct has and will continue to cause damage to Plaintiffs in an amount to be proven at trial. Unless permanently restrained and enjoined by the Court, Defendants will continue to violate the alleged provisions of the DMCA.

COUNT II

(Facilitating the Unauthorized Decryption and Reception of Satellite Signals in Violation of the Communications Act, 47 U.S.C. § 605(a))

52. Plaintiffs incorporate by reference paragraphs 1 through 51 as if set forth herein.

53. Defendants were and are assisting others, namely those purchasing "Coolsat" branded FTA Receivers and downloading the corresponding Pirate Software from websites, to intercept and receive ECHOSTAR's encrypted satellite transmissions without authorization and for their own benefit in violation of 47 U.S.C. § 605(a).

54. Defendants were and are assisting, directly or indirectly, with the design, manufacture, development, assembly, modification, solicitation, and/or distribution of "Coolsat" branded FTA Receivers and corresponding Pirate Software with knowledge, or having reason to

know, that such devices and technology are used primarily to assist in the unauthorized interception and decryption of direct-to-home satellite services in violation of 47 U.S.C. § 605(a).

55. Defendants violated 47 U.S.C. § 605(a) of the Communications Act willfully and for the purpose of direct or indirect commercial advantage or private financial gain.

56. Defendants' misconduct has and will continue to cause damage to Plaintiffs in an amount to be proven at trial. Unless permanently restrained and enjoined by the Court, Defendants will continue to violate the alleged provisions of the Communications Act.

COUNT III

(Manufacture and Sale of Signal Theft Devices and Technology in Violation of the Communications Act, 47 U.S.C. § 605(e)(4))

57. Plaintiffs incorporate by reference paragraphs 1 through 56 as if set forth herein.

58. Defendants were and are engaged in the business of designing, manufacturing, developing, assembling, modifying, importing, exporting, selling, or otherwise distributing "Coolsat" branded FTA Receivers and corresponding Pirate Software to facilitate the illegal use and reception of ECHOSTAR's encrypted satellite transmissions without authorization in violation of 47 U.S.C. § 605(e)(4).

59. Defendants were and are assisting, directly or indirectly, with the design, manufacture, development, assembly, modification, solicitation, and/or distribution of "Coolsat" branded FTA Receivers and the corresponding Pirate Software with knowledge, or having reason to know, that such devices and technology were and are used primarily to assist in the unauthorized interception and decryption of direct-to-home satellite services in violation of 47 U.S.C. § 605(e)(4).

60. Defendants violated 47 U.S.C. § 605(e)(4) of the Communications Act willfully and for the purpose of direct or indirect commercial advantage or private financial gain.

61. Defendants' misconduct has and will continue to cause damage to Plaintiffs in an amount to be proven at trial. Unless permanently restrained and enjoined by the Court, Defendants will continue to violate the alleged provisions of the Communications Act.

///

COUNT IV

(Unauthorized Interception of Electronic Communications in Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2520(a))

62. Plaintiffs incorporate by reference paragraphs 1 through 61 as if set forth herein.

63. Defendants were and are intentionally intercepting ECHOSTAR's encrypted satellite transmissions in violation of the Electronic Communications Privacy Act ("Wiretap Act"), 18 U.S.C. § 2520(a), by using "Coolsat" branded FTA Receivers, components, and corresponding Pirate Software, which is prohibited by section 2511(1)(a) of the Wiretap Act.

64. Defendants knew that the interception of ECHOSTAR's encrypted satellite signals was and is illegal and prohibited.

65. Defendants violated sections 2511(1)(a) and 2520(a) of the Wiretap Act for a tortious or illegal purpose, or for purposes of direct or indirect commercial advantage or private financial gain.

66. Defendants' misconduct has and will continue to cause damage to Plaintiffs in an amount to be proven at trial. Unless permanently restrained and enjoined by the Court, Defendants will continue to violate the alleged provisions of the Wiretap Act.

COUNT V

(Unfair Competition in Violation of California Business & Professions Code § 17200)

67. Plaintiffs incorporate by reference paragraphs 1 through 66 as if set forth herein.

68. Defendants' promotion, distribution, and provision of piracy devices, components, and technology which are primarily designed to circumvent Plaintiffs' Security System and steal DISH Network Programming constitute unlawful and unfair business acts and practices within the meaning of California Business and Professions Code § 17200 *et seq.*

69. Defendants' unlawful business acts and practices, as alleged herein, violate provisions of the Digital Millennium Copyright Act, 17 U.S.C. § 1201 *et seq.*, the Communications Act of 1934, as amended, 47 U.S.C. § 605 *et seq.*, and the Electronic Communications Privacy Act, 18 U.S.C. § 2511 *et seq.*

///

70. Defendants' business acts and practices, as alleged herein, are unfair because any utility gained by Defendants' misconduct is outweighed by the gravity of the consequence to Plaintiffs and the general public, and/or Defendants' misconduct is immoral, unethical, oppressive, unscrupulous, or substantially injurious to Plaintiffs and the general public.

71. Defendants' unlawful and unfair business acts and practices have proximately caused and will continue to cause substantial and irreparable injury to Plaintiffs, including loss of current and/or potential subscribers, dilution of goodwill, confusion of potential customers, and injury to reputation.

72. Unless permanently restrained and enjoined by the Court, Defendants' wrongful business activities will continue to violate the alleged unfair competition laws of California.

COUNT VI

(Unjust Enrichment)

73. Plaintiffs incorporate by reference paragraphs 1 through 72 as if set forth herein.

74. Defendants intentionally usurped for themselves, and through others acting in concert, Plaintiffs' trade secrets, proprietary information, revenues, and other property rights for the purpose of, among others, enhancing the commercial value of Defendants' products and technology by effectuating, and assisting others in effectuating, the circumvention of Plaintiffs' Security System.

75. Upon information and belief, discovery will show that Defendants are currently in possession of: (1) Plaintiffs' trade secrets and proprietary information, including but not limited to, portions of the security keys and codes contained within the Nagra Software that are used to illegally circumvent Plaintiffs' Security System; (2) devices, components, and technology designed to intercept and decrypt ECHOSTAR's satellite signals; and (3) monies or other proceeds unlawfully obtained through the promotion, distribution, and sale of piracy devices, components, and technology designed to steal DISH Network Programming.

76. As a direct and proximate result of the unlawful and improper acts alleged herein, Defendants have been unjustly enriched by garnering lost profits and goodwill from

ECHOSTAR. The amount of profits unjustly realized by Defendants cannot be readily ascertained by ECHOSTAR without an accounting of Defendants' business records.

77. Unless permanently restrained and enjoined, Defendants' misconduct has and will continue to unjustly enrich Defendants and cause further damage to ECHOSTAR in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs ECHOSTAR and NAGRASTAR seek judgment against Defendants as follows:

A. For a grant of permanent injunctive relief restraining and enjoining Defendants, and their employees, agents, representatives, attorneys, and all persons acting or claiming to act on their behalf or under their direction or authority, and all persons acting in concert or in participation with them, from:

(1) offering to the public, providing, or otherwise trafficking in any FTA Receivers, Pirate Software, or any other device, component, or technology, or part thereof, through the www.fortecfiles.com, www.abadss.com, and www.f2atv.com websites, any other Internet website, or in any other way that:

(a) is primarily designed or produced for the purpose of circumventing Plaintiffs' Security System, including the encryption and access control protection contained in the software on ECHOSTAR's Access Cards, or any other technological measure adopted by Plaintiffs that effectively controls access to copyrighted Programming on the DISH Network platform;

(b) have only a limited commercially significant purpose or use other than to circumvent Plaintiffs' Security System, including the encryption and access control protection contained in the software on ECHOSTAR's Access Cards, or any other technological measure adopted by Plaintiffs that effectively controls access to copyrighted Programming on the DISH Network platform;

(c) is knowingly marketed by Defendants and/or others acting in concert with Defendants for use in circumventing Plaintiffs' Security System, including the

encryption and access control protection contained in the software on ECHOSTAR's Access Cards, or any other technological measure adopted by Plaintiffs that effectively controls access to copyrighted Programming on DISH Network; and

(2) assembling, modifying, selling, and/or distributing any FTA Receivers or Pirate Software knowing or having reason to know that such device or software is primarily of assistance in the unauthorized decryption of direct-to-home satellite services through the www.fortecfiles.com, www.abadss.com, and www.f2atv.com websites, any other Internet website, or in any other way; and

(3) assisting others in receiving (including assistance offered by providing hypertext links or banner advertising) ECHOSTAR's electronic communications without ECHOSTAR's authorization through the www.fortecfiles.com, www.abadss.com, and www.f2atv.com websites, any other Internet website, or in any other way.

B. For an Order impounding all electronic copies of Pirate Software, FTA Receivers, or other circumvention or signal theft technology, components, or devices in the custody or control of Defendants or related entities that the Court has reasonable cause to believe were involved in a violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201 *et seq.*

C. For an Order directing Defendants to preserve and maintain all records, in any form (including electronic form), that evidence, refer, or relate to: FTA Receivers, Pirate Software, communications or correspondence with suppliers of software, hardware, or other equipment or know-how concerning satellite television piracy, including any dealer, distributor, or manufacturer of FTA Receivers.

D. Award Plaintiffs the greater of its actual damages together with any profits made by Defendants that are attributable to the violations alleged herein, or statutory damages in the amount of up to $100,000 for each violation of 47 U.S.C. § 605(e)(4), pursuant to 47 U.S.C. § 605(e)(3)(C)(i).

E. Award Plaintiffs the greater of its actual damages together with any profits made by Defendants that are attributable to the violations alleged herein, or statutory damages in the

amount of up to $2,500 for each violation of 17 U.S.C. §§ 1201(a)(2) and 1201(b)(1), pursuant to 17 U.S.C. §§ 1203(c)(2) and 1203(c)(3)(A).

F. Award Plaintiffs the greater of its actual damages together with any profits made by Defendants that are attributable to the violations alleged herein, or statutory damages in the amount of $100 per day for each violation of 18 U.S.C. § 2511(1) or $10,000, pursuant to 18 U.S.C. § 2520(c)(2).

G. Award Plaintiffs punitive damages afforded by law pursuant to 18 U.S.C. § 2520(b)(2), and in equity for unjust enrichment.

H. For an accounting and restitution by Defendants of all gain, profit, and advantages derived from Defendants' unlawful and unfair business acts and practices.

I. For an award of Plaintiffs' costs, reasonable attorneys' fees, and investigative fees.

J. For pre- and post-judgment interest on all profits and damages granted by this Court in accordance with the law.

K. For such other and further relief as the Court deems just and proper.

DATED: December 3, 2007

Respectfully submitted,

DLA PIPER US LLP

By: _____
ROY K. McDONALD
STEPHEN A. CHIARI

Attorneys for Plaintiffs
ECHOSTAR SATELLITE L.L.C.,
ECHOSTAR TECHNOLOGIES CORPORATION
and NAGRASTAR L.L.C.

DEMAND FOR JURY TRIAL

Plaintiffs ECHOSTAR SATELLITE L.L.C., ECHOSTAR TECHNOLOGIES CORPORATION, AND NAGRASTAR L.L.C., by their undersigned counsel, hereby demand a trial by jury in this action.

DATED: December 3, 2007

Respectfully submitted,

DLA PIPER US LLP

By: _____
ROY K. McDONALD
STEPHEN A. CHIARI

Attorneys for Plaintiffs
ECHOSTAR SATELLITE L.L.C.,
ECHOSTAR TECHNOLOGIES CORPORATION
and NAGRASTAR L.L.C.